

الصين.. وأمريكا.. والجيل الخامس..

التنين الصيني وفن إخضاع العدو دون قتال

أثارت القيود التي فرضتها الولايات المتحدة الأمريكية مؤخرًا، وألزمت بها بعض الشركات الأمريكية بمقاطعة شركة "هواوي"، والتي كان من أبرزها منع هواوي من استخدام نظام التشغيل أندرويد، وتطبيقاته بسبب ما اعتبرته "مخاوف تتعلق بالأمن القومي الأمريكي" الجدل حول طبيعة الصراع الدائر بين البلدين.. وقد نشرت « لغة العصر » في عددها رقم 212 الصادر في أغسطس 2018 تقريرًا يتناول المعلومات التي أثّرت بحجم الاستثمارات الضخمة التي سيولدها الجيل الخامس طبقًا لتقديرات شركة IHS للأبحاث حيث توقعت أن يصل حجمها إلى حوالي 12.3 تريليون دولار (12 ألف مليار و 300 مليار دولار أمريكي). وسنتطرق في هذا التقرير إلى أبعاد أكثر عمقا تتعلق بحجم الصراع الذي لا يتعلق بالولايات المتحدة والصين فقط، بل تتداخل في تعقيداته عشرات الدول الأخرى، ولا يشمل شركة "هواوي" فقط، بل يدخل في نطاقه عدة شركات صينية أخرى.

أشرف شهاب

تتركز المخاوف الحقيقية أو المتصورة لمعظم الدول من شركات التكنولوجيا الصينية بشكل عام، حول طبيعة العلاقات بين تلك الشركات وأجهزة الاستخبارات الصينية، التي يعززها القول بأن البيئة السياسية والقانونية الصينية تفرض على تلك الشركات التعاون مع وكالات الاستخبارات، وبالتالي، الشعور بأن استخدام الحلول التقنية التي تقدمها شركة "هواوي" سيغني ضمنيًا الاعتماد التام على معدات يمكن أن تتحكم فيها أجهزة المخابرات الصينية والجيش سواء في أوقات السلم أو الحرب.

التنين الصيني يأخذ زمام المبادرة

نجحت شركات التكنولوجيا الصينية على مدى العقود القليلة الماضية في امتلاك زمام المبادرة التكنولوجية وقيادة العالم تقنيًا، بسبب تبنيها لسياسات تعتمد على الإبداع، والابتكار والجودة الفائقة بشكل ملحوظ، بالإضافة إلى انخفاض التكلفة. ويبدو أن هذا التفوق التقني الصيني قد أثار فزع الغرب من الوقوع تحت هيمنة التنين الصيني الذي لم يخف نيته السعي بنشاط للتفوق، ومن ثم الحصول على نفوذ عالمي أقوى، مما يثير مخاوف مستقبلية بأن ذلك التفوق يحمل في طياته تهديدات على الأمن القومي والاقتصادي والاجتماعي لتلك الدول يؤدي في نهاية الأمر إلى زعزعة استقرارها خصوصًا مع شكواهم الدائمة من أن الصين تعتمد سياسات تجسس سيبرانية، وتنتهك حقوق الملكية الفكرية.

الجيل الخامس ليس مجرد تقنية

في ظل المخاوف الغربية المتأصلة تاريخيًا تجاه الصين، يأتي تملكها لزمام القيادة في تقنيات الجيل الخامس كعنصر إضافي يزيد الأمور اضطرابًا، إذ أن طبيعة وإمكانات الجيل الخامس لا تقتصر على كونه مجرد تقنية جديدة، واعدة، توفر جودة فائقة، وإمكانات مبتكرة. فشبكات الجيل الخامس تمتلك في طياتها إمكانية أن تصبح النظام العصبي الرقمي للمجتمعات المعاصرة، ومع عدم وجود ضمانات بأن تكون التكنولوجيا آمنة تمامًا، والوضع يعين الاعتبار مخاطر حدوث ثغرات أمنية غير متوقعة يمكن استغلالها من قبل جهات معادية. فإن قدرات الصين المعروفة، وميلها للاستفادة من هذه الميزات، يجعل مسألة نشر الجيل الخامس أكثر من مجرد مسألة فنية يمكن النظر إليها على ضوء اعتبارات محددة، لأن الاختيارات التكنولوجية يمكن أن تكون لها آثار أمنية اقتصادية وقومية على حد سواء.

وتعتقد الدول الغربية أنه عند النظر في الإمكانيات الهائلة التي تحملها تقنيات الجيل الخامس، فإنه لا يمكن بأي حال من الأحوال الفصل بين منظور الاستخدامات المدنية أو الدفاعية، إذ أن منظمات الأمن والدفاع الوطنية

نشر "مركز التميز للدفاع السيبراني التابع لمنظمة حلف شمال الأطلسي" The NATO Cooperative Cyber Defence Centre of Excellence-CCD-COE وهو مركز بحثي للدفاع السيبراني معتمد من حلف شمال الأطلسي "الناتو"، يركز على الأبحاث والتدريب في نهاية شهر مارس الماضي تقريرًا تحت عنوان: "هواوي والجيل الخامس والصين كتهديد أمني" Huawei, 5G and China as a Security Threat. ويشير التقرير إلى أن العقوبات التي فرضتها كل من أمريكا، وأستراليا، ونيوزيلندا، واليابان، وجمهورية التشيك على استخدام حلول الجيل الخامس للاتصالات المحمولة التي تقدمها شركة "هواوي" أثارت حفيظة عدد من المتحمسين لتقنيات الجيل الخامس الذين يعتقدون أن من شأن تلك الإجراءات إبطاء نشر شبكات الجيل الخامس على مستوى العالم.



الصيني المتصاعد في المنظمات الدولية المعنية بوضع معايير الاتصالات العالمية، كالاتحاد الدولي للاتصالات ITU، ومشروع شراكة الجيل الثالث 3G Partnership Project.

اقتصاديات الحجم

يعد حجم السوق الصيني الأضخم في العالم من حيث عدد السكان 1.42 مليار نسمة (مليار و420 مليون نسمة)، من العوامل المؤثرة في نمو الشركات الصينية بشكل كبير، بالإضافة إلى السياسات التي تتبعها الحكومة الصينية لتشجيع الشركات، حيث أعلنت الحكومة الصينية مرارا عزمها أن تصبح قوة عظمى في التكنولوجيا الرقمية. ووضعت عام 2006 استراتيجية طويلة الأجل للابتكار كان من بين أهدافها الابتكار التكنولوجي، وفك الارتباط عن الغرب. وتم دعم هذا الجهد من بتركيز الاستثمارات الحكومية في مجال البحث والتطوير التكنولوجي. ومن خلال تقييد وصول الشركات الغربية إلى السوق الصينية، تمكنت الصناعة الصينية من الاستفادة من حجم السوق المحلي، دون منافسة أجنبية (تسيطر الشركات الصينية على 75٪ من السوق الصيني). ومع النجاح الذي لقيته الاستراتيجية الوطنية الصينية، تم تعزيزها باستحواذ رأس المال الصيني على العديد من شركات التكنولوجيا والبنية التحتية الأمريكية والغربية.

أنشطة هواوي

لا يوجد حتى هذه اللحظة أي دليل، على الأقل علنا، على وجود نقاط ضعف كبيرة في التقنيات التي تقدمها شركة "هواوي" ولا توجد أي أدلة ملموسة على تورطها في أعمال تجسس. ومع ذلك، فقد تم إلقاء اللوم على الشركة مرارا وتكرارا بسبب التجسس الصناعي (قضية Cisco عام 2003 وقضية T-Mobile عام 2014)، وحتى المزاعم بأن الحكومة الصينية تنتهك العقوبات الاقتصادية الدولية ضد إيران وكوريا الشمالية، لا علاقة قوية بينها وبين الاتهامات الموجهة لشركة "هواوي". ومع ذلك، تم توجيه الاتهامات لشركة "هواوي" بالتجسس، وربطت تقارير خاصة بالاستخبارات الأسترالية العام الماضي بين موظفي "هواوي" وعمليات تجسس عن طريق الحصول على رموز دخول والتسلل إلى شبكات محلية. كما احتجرت كل من كندا وبولندا في الأشهر الأخيرة اثنين من مسؤولي شركة "هواوي"، بينهما ابنة مؤسس ورئيس شركة "هواوي". ونفت شركة "هواوي" عدة مرات على لسان عشرات المسؤولين من أبرزهم مؤسس الشركة ورئيسها "رن تزنغفي"، الذي أكد مرارا وتكرارا أن أسهم الشركة مملوكة من قبل موظفين، وأنها ليست ملكا لأي حكومة، وأنها لم تستخدم معادنها للتجسس أو التخريب في بلدان أخرى. كما نفى بشكل قاطع أن تكون "هواوي" قد قدمت أو قامت في أي وقت مضى بتقديم معلومات عن العملاء لأي حكومة أو مؤسسة. وإثباتا لحسن نيتها قامت "هواوي" بإنشاء عدة مراكز لتقييم الأمان Huawei Cyber Security Evaluation Centre-HCSEC الخاص بمنتجاتها في المملكة المتحدة، وألمانيا، ومؤخرا في العاصمة البلجيكية بروكسل لتزويد الشركاء بفرصة لتقييم منتجات الشركة عن كثب والتأكد من عدم وجود أي أنشطة مشبوهة، بل، وأتاحت لهم "الكود المصدري" لمنتجاتها للمزيد من إثبات حسن النية. وتؤكد الشركة دائما في بياناتها أنها: "شركة التكنولوجيا الأكثر دقة في العالم". ويعتبر "مركز التقييم" الذي أنشأته شركة "هواوي" في المملكة المتحدة HCSEC من خلال مجلسه الرقابي الذي تسيطر عليه "هيئة الأمن السيبراني" National Cyber Security Centre-NCSC والذي يتبع Gov-ernment Communications Headquarters (GCHQ) وهي وكالة تابعة لجهاز الاستخبارات والأمن البريطانية، فريدا حتى الآن في نموذج عمله. لدرجة أن المراكز المماثلة التي أُنشئت في ألمانيا وبلجيكا تفتقر إلى إشراف مماثل.

وعلى الرغم من كل تلك الضمانات التي قدمتها "هواوي" إلا أن الحكومات الأوروبية تعتقد أنه حتى في حالة عدم وجود علاقة رسمية بين شركات التكنولوجيا الصينية والحكومة الصينية، فإن البيئة القانونية الصينية مواتية وتسمح للحكومة الصينية باستخدام الشركات الخاصة وتكنولوجياها كأدوات للتجسس.

ليست هواوي فقط

كما يشير تقرير CCDCOE إلى أنه على الرغم من التركيز الشديد على شركة "هواوي" كمتهمة، بسبب قدراتها المتطورة في تقنيات الجيل الخامس،

تستخدم إلى حد كبير البنية التحتية المدنية، وتمتلك التفويضات اللازمة للتدخل لحمايتها أثناء الأزمات. وبما أن المزيد من التقنيات "الرقمية" أو "الذكية" تجد طريقها إلى العمليات العسكرية، فإن من الصعب التفكير في إنشاء بنية تحتية رقمية موازية منفصلة مخصصة للاستخدامات الدفاعية.

الجيل الخامس والتهديدات الأمنية

يوفر الجيل الخامس من الاتصالات المحمولة سرعات أكبر في نقل البيانات ووقت استجابة أقل (استجابة أفضل) وإمكانية الاتصال في وقت واحد بملايين الأجهزة "إنترنت الأشياء". وبالتالي فإن سرعة تطبيق ونشر تقنيات الجيل الخامس سوف يسرع من تقدم تقنيات الروبوتات وعمليات الأتمتة، وسيديم بشكل متقدم تقنيات "الواقع الافتراضي" Virtual Reality-VR و"الواقع المعزز" Augmented Reality-AR، و"الذكاء الاصطناعي" Artificial Intelligence-AI والتعلم الآلي Machine Learning-ML. وهو ما يعني أننا أمام تقنية ستقوم بتغيير المشهد العالمي للأجهزة والتطبيقات بشكل جذري، وستقوم بتحويل المجتمعات إلى مجتمعات رقمية بالكامل، وهي تحولات يصعب تخيلها اليوم. وفي إطار التهديدات القائمة ولكنها ليست واقعية أو مدعومة بأدلة ملموسة، تعتقد أمريكا وحليفاتها من الدول الغربية أن قيام الجيل الخامس بربط مليارات الأجهزة بالشبكات يعني زيادة هائلة في الأهداف المحتملة وفي وسائل التجسس، ناهيك عن إمكانية استخدامها كمنصات استخبارات عن طريق التقاط الإشارات الناشئة عنها لتمكين جمع وتحليل بيانات القياس عن بعد على نطاق واسع.

كما تقلل تقنية الجيل الخامس من الفصل بين شبكات الاتصالات الطرفية والشبكات الأساسية، مما يعني أنه الصعب الحد من تأثير البائعين ليس فقط على الشبكات الأساسية بل على الشبكات الطرفية أيضا، مما يعني أن أي تهديد محتمل للشبكة سيكون تهديدا شاملا لكامل الشبكة، وفي هذه الحالة سيكون من الصعب، بل ربما من المستحيل التراجع عن استخدام الشبكات التي تم تركيبها، لأن أي محاولة لتغيير التقنية المعتمدة سيكون معناه الإضرار إلى تغيير هيكلية الشبكة بالكامل، وهو أمر معقد، ومكلف، ويستغرق وقتا طويلا.

لماذا هواوي؟

يشير التقرير الذي أشرنا إليه إلى أن صعود نجم شركة "هواوي" على المستوى العالمي يعتبر مثالا حيا على السياسات التي اتبعتها الصين للتفوق التكنولوجي، وريادة العالم في هذا المجال. فقد شهدت السنوات القليلة الماضية نمو الشركة لتصبح أكبر شركة لتصنيع معدات الاتصالات على مستوى العالم. وفي عام 2018 تفوقت "هواوي" على شركة "أبل" لتصبح ثاني أكبر منتج للهواتف الذكية بعد شركة "سامسونج" الكورية الجنوبية. وتعد شركة "هواوي" حاليا الشركة الوحيدة التي يمكنها إنتاج جميع عناصر شبكة الجيل الخامس، على نطاق واسع وبتكلفة معقولة، والأهم من ذلك بلا منافسة حقيقية، إذ أن أقرب منافسيها "نوكيا" و"إريكسون" ما زالا غير قادرين حتى اللحظة على تقديم بديل قابل للتطبيق، مما أفسح المجال واسعا أمام هواوي للسيطرة على سوق الاتصالات اللاسلكية للجيل الخامس تقريبا، وأتاح لها أن تتعاون مع كبريات شركات الاتصالات في عدد من البلدان الأوروبية، وفي جميع أنحاء العالم.

براءات الاختراع كعنصر تفوق

يرجع الفضل في تفوق "هواوي" وغيرها من شركات الاتصالات الصينية الأخرى في تقنيات الجيل الخامس إلى تاريخ طويل من الإبداع والابتكار، والتطوير، حيث تمتلك الشركات الصينية نسبة كبيرة من براءات الاختراع الأساسية للجيل الخامس. وتمتلك الصين حاليا ما يقرب من 10٪ من حقوق الملكية الأساسية لتقنيات الجيل الخامس. وتأتي "هواوي" على رأس الشركات في نسب براءة الاختراع، تليها شركة ZTE. بالإضافة إلى النفوذ

فن الحرب الأسمى
هو إخضاع العدو دون قتال

من تزو

الجنرال الصيني والاستراتيج العسكري والكاتب والفيلسوف



الصين والحقوق الفردية

تختلف المقاربات الصينية والغربية تجاه الحقوق الفردية اختلافا جذريا. فعلى سبيل المثال يتخذ الاتحاد الأوروبي موقفا صارما بشأن حماية الخصوصية الفردية، كما يتضح من خلال تطبيق اللائحة العامة لحماية البيانات (GDPR) ما قد يعنى تفضيل الحقوق الخاصة على حقوق الدولة. فى حين يسود الاعتقاد بأن الصين تعمل بمنهج مختلف يفضل مصلحة الدولة على المصالح الخاصة، ومن هنا ينشأ تخوف آخر يقول إنه على الرغم من أن شركات مثل "هاواي" تخضع للقوانين المحلية للبلدان التي تعمل فيها، إلا أن المصالح المتداخلة والمتشابكة للشركة يمكن أن تضعها فى منطقة اختصاصات قضائية متشابكة قد تجبر الشركات الصينية فى نهاية المطاف على التعاون مع وكالات الاستخبارات الصينية. ويدعم هذه المخاوف تقرير التحقيق الذي أجرته لجنة الاستخبارات بمجلس النواب الأمريكى فى عام 2012 حيث توصل التقرير إلى ما مفاده فشل شركة "هاواي" فى "الكشف عن تفاصيل تعاملاتها مع الجيش أو أجهزة المخابرات الصينية" ورفضها "تقديم إجابات واضحة عن آليات صنع القرار داخل الشركة". كما قال التقرير إن اللجنة لم تتلق أى معلومات تقريبا عن دور لجنة الحرب الشيوعى الصينى فى شركة "هاواي" أو تعاونها مع الحكومة الصينية.

قيود القانون الدولي

نظرا لأن الخطر الرئيسى المتمثل فى استخدام التكنولوجيا الصينية ينبع من التأثير الذى يمكن أن تمارسه الحكومة الصينية على الشركات الصينية. ومع الإقرار بأن سلطة الصين السيادية على شئونها الداخلية تعنى أنها حرة فى فرض التزامات على صناعاتها، بما فى ذلك لغرض التعاون الاستخباراتي. فإن الجانب الآخر من ممارسة حقوق السيادة، يعنى أيضا أن الدول الغربية حرة من حيث المبدأ فى حظر المنتجات الصينية، بشرط احترام التزاماتها الناشئة بموجب ترتيبات التجارة الدولية، خاصة الاتفاقية العامة لمنظمة التجارة العالمية بشأن التعريفات الجمركية والتجارة (GATT) التى تغطى التجارة الدولية فى البضائع.

وبما أن شبكات الاتصالات الأساسية بنية تحتية أساسية، وبالتالي فهي مصلحة وطنية أساسية، لها آثار على الأمن القومى. وبالتالي فإن اعتماد تكنولوجيا "هاواي" أو ZTE أو أى شركة صينية أخرى كشبكات اتصالات أساسية يعنى أنها ستصبح جزءا من البنية التحتية الأساسية للاتصالات فى عشرات البلدان. وهذه البنية التحتية سيتم الاعتماد عليها لأداء مجموعة من الخدمات الأساسية، والوظائف الاجتماعية والاقتصادية. وهذا يعنى أن نشر تكنولوجيا "هاواي" سيجعلها تتغلغل فى مكونات مهمة فى الأنظمة ذات الأهمية الاستراتيجية للمجتمعات، بما فى ذلك الخدمات الأمنية والعسكرية، خصوصا إذا تطلب الأمر الاعتماد على تلك التكنولوجيا ولو بشكل جزئى أثناء الأزمات.

التبعية الرقمية

إن أهمية البنية التحتية الأساسية لعمل المجتمع تجعل من نشر البنية التحتية للاتصالات قرارا استراتيجيا ليس فقط لمشغلي الاتصالات، ولكن بالنسبة للأمة بأكملها، خاصة وأن المتوقع أن تؤدي تقنيات الجيل الخامس إلى نمو هائل فى الخدمات التى تدعم إنترنت الأشياء (ليس فقط درجة التبعية الرقمية للمجتمعات المعاصرة بل طابعها ذاته). لذلك، قد يكون للحادث

إلا أن القضية لا تتعلق بشركة "هاواي" فقط. فالعديد من الدول تشعر بالقلق أيضا بشأن العديد من الشركات الصينية الأخرى المصنعة لتكنولوجيا الاتصالات، ومن أهم تلك الشركات شركة ZTE وهى واحدة من الشركات الرائدة فى تصنيع معدات الاتصالات فى الصين، وإحدى الشركات الرائدة فى مجال توفير معدات الشبكات. وتشمل قائمة منتجاتها الرئيسية الشبكات الأساسية، وشبكات النقل، وشبكات الوصول اللاسلكى، والثابت، والحوسبة السحابية، وحلول الطاقة. وفى عام 2017 تم اتهام ZTE بتصدير التكنولوجيا الأمريكية بشكل غير قانونى إلى إيران وكوريا الشمالية فى انتهاك للعقوبات الاقتصادية. وفى أبريل 2018، فرضت وزارة التجارة الأمريكية حظر تصدير لمدة 7 سنوات على منتجات ZTE إلى الولايات المتحدة. وتم رفع ذلك الحظر فى يوليو 2018 بعد قيام ZTE بحل مجلس الإدارة، وموافقتها على دفع غرامات إضافية وإنشاء فريق امتثال داخلى للعقوبات الدولية على إيران وكوريا الشمالية. وبالإضافة إلى "هاواي" و ZTE تشمل قائمة الشركات الصينية الأخرى شركات مثل: Hytera Communications Corporation و Hangzhou Hikvision و Dahua Technology وتعد شركة Hytera ثانى أكبر شركة مصنعة لمحطات توزيع الطيف الترددى عالميا حيث تمتلك 13 % من حصة السوق العالمى. وهى تنتج أنظمة DMR و LTE و MPT-1327 بالإضافة إلى أنظمة TETRA التى تم تصميمها خصيصا للاستخدام من قبل الوكالات الحكومية، وخدمات الطوارئ وشبكات السلامة العامة وخدمات النقل (السكك الحديدية على وجه الخصوص) والاستخدامات العسكرية. أما شركتا Hikvision و Dahua فهما المزودان الصينيان لمنتجات المراقبة بالفيديو، وهما يحتلان المركز الأول والثانى من حيث الحصة السوقية على مستوى العالم. وجميع هذه الشركات الثلاث تم حظر استخدام تكنولوجياها فى الشبكات الحكومية بموجب القانون الأمريكى.

التجسس والتأثير

يشير تقرير CCDCOE إلى أن المخاوف الأمنية الغربية الأمريكية والأوروبية بشأن استخدام التكنولوجيا الصينية قديمة، وتزايدت مع بزوغ نجم الصين، وتساعد موقعها فى الأسواق العالمية. كان المسنولون الحكوميون الغربيون والمجتمع الأمنى قلقين بشأن إمكانية استخدام الحكومة الصينية والجيش الصينى للتكنولوجيا التى تنتجها الشركات الصينية للتجسس على المستخدمين، بسبب ما أسماه التقرير تمتع الصين بسعة سيئة فى مجال التجسس الصناعى، وكذلك التعاون الوثيق بين الحكومة والصناعة الصينية فى "استهداف المؤسسات الأكاديمية والصناعة والمرافق الحكومية لغرض جمع الأسرار التكنولوجية".

وهناك مجموعة طويلة من الأمثلة التى يتم التدليل بها على تلك المزايع باستخدام القدرات السيبرانية الحكومية والعسكرية لأغراض التجسس الاقتصادى. وفى عام 2013، أصدرت شركة Mandiant (شركة أمن سيبرانى أمريكية) تقريراً أشارت فيه إلى حملة تهديد متواصل لسنوات متعددة، ربطت فيه بين مجموعة تسمى: APT-1 وجيش التحرير الشعبى الصينى. وقامت باستعراض ما قالت إنه قيام تلك المجموعة بسرقة منهجية لبيانات سرية من أكثر من 140 منظمة تعمل فى صناعات متعددة. وفى شهر ديسمبر الماضى 2018، أعلنت المملكة المتحدة وحلفاؤها أن مجموعة معروفة باسم APT-10 تعمل نيابة عن وزارة أمن الدولة الصينية للقيام بحملة سيبرانية ضارة تستهدف الملكية الفكرية والبيانات التجارية الحساسة فى أوروبا وآسيا والولايات المتحدة الأمريكية. أما فى الولايات المتحدة الأمريكية، فمن بين جميع قضايا التجسس الاقتصادى التى نظرت فيها وزارة العدل بين عامى 2011 و 2018 كانت الصين عنصرا مشتركا بنسبة 90 %.

البيئة القانونية والسياسية فى الصين

يشير تقرير CCDCOE إلى أن قانون الاستخبارات الوطنى الصينى الصادر عام 2016 يشترط على جميع الشركات، دعم وتقديم المساعدة والتعاون فى عمل الاستخبارات الوطنية، وضمان سرية أى عمل استخبارى وطنى يحيطون به علما. وتحمى الدولة الأفراد والمنظمات التى تدعم وتعاون وتتعاون فى عمل الاستخبارات الوطنية. وعلى نفس المنوال، يفرض قانون مكافحة التجسس الصينى لعام 2014 التزامات على "المنظمات والأفراد ذوى الصلة" بتقديم المعلومات أو التسهيلات أو غيرها من المساعدات، ويؤكد للمنظمات والأفراد المعنيين بأنه "يجب ألا يرفضوا" التعاون. وهذه المواد القانونية تثير مخاوف عميقة فيما يتعلق بوضع الشركات الصينية فى حالة رأت الدولة الصينية أن ذلك التعاون ضرورى طبقا لمفهومها المتمثل فى الحفاظ على أمن الدولة الصينية.

التعاون. ومن أمثلة ذلك التعاون كما أشرنا مراكز الأمن السيبراني في المملكة المتحدة وألمانيا وبلجيكا. الذي تم إنشاؤه عام 2010 لتقييم أجهزة وبرامج "هواوي"، ويخضع لرقابة هيئة الأمن السيبراني التي هي جزء من وكالة الاستخبارات والأمن البريطانية، حيث يتم إصدار تقارير منتظمة عن النتائج التي يتم التوصل إليها، وآخرها في يوليو 2018 وقد أدرك رئيس هيئة الأمن السيبراني مؤخرا أن هذه الرقابة الرسمية المفصلة، تعني أن نظام المملكة المتحدة هو نظام الرقابة الأشد والأكثر صرامة في العالم على "هواوي"، وأنه يثبت جدواه يوما بعد يوم. نفس الأمر ينطبق على المركز الذي أقامته "هواوي" في ألمانيا في نوفمبر 2018 "للتعاون مع العملاء والشركاء والمؤسسات البحثية الألمانية، وكذلك السلطات الحكومية والإشرافية"، وينطبق كذلك على "مركز الشفافية الأمنية السيبرانية" التابع للاتحاد الأوروبي في بروكسل الذي أنشأته "هواوي" في مارس 2019. وقد عرضت "هواوي" إنشاء مركز مماثل في هولندا.

حلول بديلة وتفاعلات دولية

يعد تسريع نخوض مقدمى الخدمات البديلة أحد الخيارات. فعلى سبيل المثال أبدت "كندا" منتصف يناير 2018، اهتمامها بالحلول البديلة المنافسة لتقنيات "هواوي" ونظرت بعين الاعتبار إلى التكنولوجيا التي تقدمها شركة "نوكي" من خلال قيامها بمنح الشركة 40 مليون دولار لتمويل عمليات البحث والتطوير المتعلقة بتقنيات الجيل الخامس. ويعتقد الخبراء في CCDCOE أن مثل هذه الوسائل سوف تساعد على تحفيز تنوع العروض في السوق العالمي لمنع الهيمنة غير المرغوب فيها على السوق من شركة واحدة، بغض النظر عن المنشأ، أو أي مخاطر أمنية محتملة.

وفي ديسمبر 2018 أعلنت مجموعة الاتصالات البريطانية BT Group المشغل لخدمات للاتصالات في المملكة المتحدة عن قرارها بالتخلي عن أجهزة "هواوي" لكل من الجيل الثالث والجيل الرابع الحالية، والجيل الخامس المستقبلية. وذكرت شركة الاتصالات الألمانية دويتشه تيليكونم أنها تراجع إستراتيجياتها تجاه مزودي الأجهزة والمعدات. وأعلنت شركة "أورنج" الفرنسية أنها لن تستخدم أجهزة "هواوي". وأعلنت شركة TCD، أكبر مشغل للاتصالات في الدنمارك، أنها اختارت شركة "إريكسون" كمورد لمعدات الجيل الخامس، ولكنها بررت قرارها بأنه بسبب "اعتبارات الجودة".

ليست مسألة تقنية فقط

لا يوجد حتى الآن أي دليل عام على وجود ثغرات تقنية خطيرة في أجهزة "هواوي" أو ZTE ومع ذلك، من المستحيل بشكل أساسي استبعاد عيوب التكنولوجيا المحتملة التي يمكن استغلالها في المستقبل. سواء كانت هذه التكنولوجيا صينية أو غير صينية، وسواء كانت الثغرات الأمنية نتيجة لإجراء متعمد أو قابلة للاستغلال بسبب الفشل في تصحيح البرامج أو عيوب التصنيع، أو عيوب الاستخدام السيء من جانب المستخدمين. سيظل هذا الأمر مصدر قلق لأن شراء تقنية معينة من شركة معينة يخلق درجة من الاعتماد على هذا البائع، لأن شراء التكنولوجيا الرقمية لا يقتصر على شراء "المعدات"، بل ينطوي أيضا على التزام طويل الأمد بعلاقة استراتيجية مع الشركة الموردة للمعدات، وبالنظر إلى هذه الاعتبارات المسبقة، يمكن القول إن جوهر مشكلة "هواوي" هو هل يمكن الوثوق فيها؟ وما هي الآليات التي تعتمد عليها هذه الثقة: هل هي مصداقية الشركة أو انفتاحها على عمليات التحقق أو المساءلة أو أي شيء آخر؟

هل يستطيع الغرب تحمل النتائج؟

وبكل تأكيد لا توجد ردود سهلة على هذه الأسئلة. ومن المتوقع أن يأتي قرار إغلاق باب التعاون مع "هواوي" والصين بنتائج عكسية، لأنه سيحرم أوروبا وكثيرا من الدول حول العالم من فرصة تطوير خدمات الجيل الخامس. وفي نفس الوقت فإن انعكاسات مثل هذه القرارات على الصين قد لا تكون خطيرة بالحجم المتوقع لأن الشركات الصينية، يمكنها تحمل تبعات مثل هذه القرارات بسبب ما أوضحناه مسبقا عن نطاق وحجم القوة الشرائية المتزايدة للسوق المحلية الصينية، فضلا عن انفتاح الصين ومشاركاتها النشطة مع عشرات البلدان النامية كأسواق مستقبلية في إطار مبادرة "الحزام والطريق"، التي تسعى الصين من خلالها لمزيد من خطط التعاون الواسعة ليس فقط في قطاعات الاتصالات والتكنولوجيا، بل، وفي تطوير شبكات الطرق، والسكك الحديدية، والجسور، والطيران المدني، والموانئ، والطاقة. كما أن الغرب بإحجامه عن حلول "هواوي" لا يجد على أرض الواقع الملموس بدائل مكافئة لتكنولوجيا "هواوي". والدول الغربية لن تستطيع في الغالب تحمل نتائج ما يمكن أن تسببه أزمة "هواوي" من ركود تكنولوجي، خصوصا مع الفوائد الاجتماعية والاقتصادية المتوقعة من الجيل الخامس.

السيبراني المحتمل درجات مختلفة من التأثير على الأمن القومي والمصالح الوطنية الحيوية. وبما أنه من الصعب استبعاد أي من هذه المخاطر بشكل أساسي، فإن موثوقية الشركات الموردة للشبكات كشريك لمنع وكشف الثغرات المحتملة، والتعاون في تخفيف المخاطر تنطوي على أهمية بالغة. ونظرا لتكلفة وصعوبة استبدال أو تكرار إنشاء مثل هذه البنية التحتية الأساسية، تعتقد الدول الأوروبية أن عليها موازنة المخاطر المحتملة من الشركات الموردة للبنية التحتية بشكل شامل، ومسبقا. وعلاوة على ذلك، ونظرا لديمومتها النسبية، يمكن أن يكون لقرارات نشر البنية التحتية آثار طويلة المدى على التعاون مع الشركاء الدوليين والحلفاء بسبب المخاطر المحتملة على مشاركة المعلومات الحساسة، وهو ما حذرت منه الولايات المتحدة حلفاءها في حلف "الناتو" مؤخرا.

على ضوء هذه المخاوف، اختارت عدة دول فرض قيود على استخدام التكنولوجيا الصينية في بنيتها التحتية الأساسية. بعض الدول اختارت إصدار توجيهات ملزمة لقبول أو تقييد التكنولوجيا الصينية كما في حالة الولايات المتحدة وجمهورية التشيك، وأستراليا، واليابان التي أصدرت إرشادات أمنية إلزامية تستلزم نشر معدات البنية الأساسية من مقدمى الخدمات الذين يحتمل أن تسيطر عليهم حكومات أجنبية. وفي المقابل تدخلت نيوزيلندا بقوة وأجبرت شركات الاتصالات على عدم اعتماد تقنيات "هواوي" للجيل الخامس على أساس قانون الاتصالات لعام 2013 (بموجب حق الاعتراض) بسبب "مخاطر الأمن القومي".

وتبنت الولايات المتحدة قانونا في عام 2018 يحظر شراء واستخدام منتجات الاتصالات والمراقبة الموردة من شركات صينية محددة. وتحدثت "هواوي" مؤخرا هذه الخطوة باعتبارها: "غير دستورية"، و "مقيدة للمنافسة العادلة"، ومضرة للمستهلكين الأمريكيين، لكن من المتوقع عدم قبول اعتراض "هواوي".

حبر على ورق

في المقابل اختارت بعض الدول الامتناع عن فرض قيود على "هواوي". فقد أشار رئيس المكتب الفيدرالي للأمن المعلومات (BSI) في أكتوبر 2018 إلى أن هناك حاجة إلى أدلة واضحة وجادة من أجل فرض حظر على معدات "هواوي". ومع ذلك، تغير موقف ألمانيا. وفي فبراير الماضي 2019 ألححت التقارير الصحفية إلى أن ألمانيا تطالب بعقد اتفاقية "عدم تجسس" مماثلة للاتفاقية التي عقدها الولايات المتحدة مع الصين عام 2015 (تزعّم الولايات المتحدة أن الصين تخلت عن الاتفاقية فأصبحت حبرا على ورق). وفي سلوفاكيا قال رئيس الوزراء إن بلاده لا تعتبر "هواوي" تهديدا أمنيا. وأنها بحاجة إلى دليل قبل فرض أي قيود. ونفس الموقف عبر عنه عبد الله بن عامر السوادة، وزير الاتصالات وتقنية المعلومات السعودي الذي صرح مؤخرا أن بلاده لا تعتبر أن "هواوي" تشكل تهديدا أمنيا.

مخاطر محتملة ولكن

حتى في حالة وجود تخوفات من "هواوي" وغيرها من الشركات الصينية، فإن بإمكان العديد من الدول اللجوء إلى وسائل محددة أو مخصصة للتخفيف من المخاطر، خصوصا مع إعلان "هواوي" الدائم استعدادها ورغبتها في



عبد الله بن عامر السوادة
وزير الاتصالات وتقنية المعلومات
السعودية

